Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New HIPAA Tool Means No More Excuses For Lax Security

By **Jeff Overley**

Law360, New York (April 04, 2014, 5:50 PM ET) -- A digital tool recently released by federal regulators will make compliance with data-security provisions of the Health Insurance Portability and Accountability Act far easier for smaller businesses, but that helping hand will also remove any excuse for flouting obligations and make scofflaw corporations even more vulnerable to big penalties, experts say.

The software developed by the Office of Civil Rights at the U.S. Department of Health and Human Services is geared toward modestly sized providers, insurers and clearinghouses, as well as their business associates, that often lack the expertise to perform HIPAA's mandatory assessment of risks to the confidentiality of electronic health information in their possession.

As one indication of how daunting that assessment can be, even the digital tool — intended as a simplified way to account for risks — asks more than 150 questions about company practices and when printed out includes various considerations that span almost 400 pages.

"Even for the smallest providers, this is a very complex thing," said Alisa L. Chestler of Baker Donelson Bearman Caldwell & Berkowitz PC.

It's also an expensive thing, so the tool should be a welcome relief for companies that would see spending thousands of dollars on third-party advice as a major expense.

"It could be very valuable, because they could save the cost of hiring an outside party," Haynes and Boone LLP partner Ronald W. Breaux said.

One tricky part of compliance with HIPAA's Security Rule is that while a risk analysis is required, there is no one-size-fits-all way of performing it. That affords flexibility to so-called covered entities and business associates, but it also means they can't necessarily use off-the-shelf best practices, because for their purposes, those policies may be inapplicable or incomplete.

In that respect, the digital tool may prove especially useful, because it covers lots of ground, comes straight from the mouths of regulators and allows for personalized data entry and feedback.

"The tool is important because you really do have to customize the [policies] to your operations," said Dianne J. Bourque of Mintz Levin Cohn Ferris Glovsky & Popeo PC.

The software hasn't received universally rave reviews so far; Breaux said he'd heard of bugs related to exporting and editing, and the system isn't supported by Apple Inc.'s desktop computers.

Also, just because it makes things easier doesn't mean it makes them easy. Attorneys said that going through all the steps isn't something an entity can do in one afternoon, as evidenced by the many questions and a feature allowing users to pause and return later at the same point.

"This is not a thing a provider can sit down in three hours and finish — there will be a lot of starts and stops," Chestler said.

But to the extent the tool is helpful, that could actually spell trouble for businesses that continue to lack proper risk assessments.

"If there's a tool you can use, there's really no excuse," Bourque said.

Enforcement records suggest the OCR has shied away from punitive measures when policing HIPAA compliance, preferring to educate the health care community as long as good-faith efforts at compliance are made. For example, there have been an average of about 200 data breaches annually in recent years that crossed a 500-person threshold, which triggers prompt notification of government officials. But only 16 entities have faced financial penalties since HIPAA was revised in 2009, and in virtually all those instances, there was no satisfactory risk assessment in place.

"What we see is fundamentally ... in almost all, if not all, of the enforcement actions that were publicized, they first point out the failure to have a security risk analysis," Chestler said.

Breaux noted that the OCR explicitly warned industry that using the digital tool doesn't guarantee compliance, but he said that doing so would be a powerful prophylactic against fines if regulators do ever come knocking.

“By using the tool properly, a covered entity or business associate ... will have very strong grounds from which to argue against penalties for violating the Security Rule,” Breaux said.

In addition to sending a message about risk analyses being essential, the enforcement records show that all types of entities are likely to face a day of reckoning if they don't play ball. Entities that have faced penalties related to shoddy risk assessments have included government agencies large and small, including Alaska Medicaid and Skagit County, Wash., as well as private corporations of all stripes, including insurer Blue Cross Blue Shield of Tennessee and a Massachusetts dermatology practice.

Experts say it's hard to believe that the diversity is a coincidence, suggesting that regulators have probably made a conscience effort to send a message to all stakeholders.

"They're looking to show us all that nobody is untouchable," Chestler said.

And while a lack of resources or expertise was never a good excuse for ignoring the Security Rule, the new digital tool probably confirms that nobody can expect leniency from regulators if they don't at least make some effort to respect the law.

"As a general rule in any enforcement scenario, the easier it has been made to comply, the harder it's going to be to explain noncompliance," Breaux said.

--Editing by Elizabeth Bowen and Katherine Rautenberg.
